AUTHENTICATION AND SIGNATURE METHOD FOR MESSAGES USING REDUCED SIZE OF BINARY UNITS OF INFORMATION CONTENT AND CORRESPONDING SYSTEMS

Patent number:	FR2792142
Publication date:	2000-10-13
Inventor:	GIRAULT MARC
Applicant:	FRANCE TELECOM (FR)
Classification:	
- international:	H04L9/32
- european:	H04L9/32C
Application number:	FR19990004398 19990408
Priority number(s):	FR19990004398 19990408

Also published as:

WO0062477 (A1)
EP1166496 (A1)

Abstract of **FR2792142**

The invention concerns an authentication method using a reduced number of binary units of information content and its corresponding systems. The invention is characterised in that it consists in reducing the number of binary units of information content while controlling the time taken by the entity to be authenticated to reply to the authenticating entity and in imposing that said time be less than a certain value. The security level is maintained. The invention is useful for authenticating processes (of entities, of messages) or for the signature of messages.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 792 142**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **99 04398**

(51) Int Cl[7] : H 04 L 9/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 08.04.99.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 13.10.00 Bulletin 00/41.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *FRANCE TELECOM Société anonyme* — FR.

(72) **Inventeur(s)** : GIRAULT MARC.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE D'AUTHENTIFICATION ET DE SIGNATURE DE MESSAGE UTILISANT DES ENGAGEMENTS DE TAILLE REDUITE.

(57) Procédé d'authentification utilisant des engagements de taille réduite.

Selon l'invention, on réduit la taille de l'engagement mais on contrôle le temps mis par l'entité à authentifier pour répondre à l'entité authentifiante et l'on impose que ce temps soit inférieur à une certaine valeur. Le niveau de sécurité est conservé.

Application aux procédés d'authentification (d'entités, de messages) ou de signature de messages.

FR 2 792 142 - A1

PROCEDE D'AUTHENTIFICATION ET DE SIGNATURE DE MESSAGE UTILISANT DES ENGAGEMENTS DE TAILLE REDUITE

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé d'authentification et de signature de message utilisant des engagements de taille réduite.

L'invention concerne le domaine de l'identification (c'est-à-dire l'authentification d'entité) ainsi que celui de l'authentification de message et de signature numérique de message, au moyen de techniques cryptographiques.

L'invention concerne plus précisément la cryptographie dite à clé publique. Dans ce domaine, l'entité à authentifier possède une clé secrète et une clé publique associée. L'entité authentifiante a uniquement besoin de cette clé publique pour réaliser l'authentification.

L'invention concerne plus précisément encore le domaine des procédés d'authentification dits à connaissance nulle ou sans apport de connaissance ("zero-knowledge" en anglais). Cela signifie que l'authentification se déroule suivant un protocole qui, de façon prouvée, et sous des hypothèses reconnues comme parfaitement raisonnables par la communauté scientifique, ne révèle rien sur la clé secrète de l'entité à authentifier.

L'invention trouve une application dans tous les systèmes où l'on veut authentifier des entités ou des messages, ou signer des messages, et plus particulièrement dans les systèmes où le nombre de bits

transmis et/ou stockés constitue un paramètre critique. C'est notamment le cas des cartes à microcircuit standard ou à bas coût, non pourvues d'un coprocesseur arithmétique (appelé souvent cryptoprocesseur) pour accélérer les calculs cryptographiques.

Une application typique de l'invention est le porte-monnaie électronique, qui requiert un très haut niveau de sécurité, tout en excluant l'usage d'un cryptoprocesseur, soit pour des raisons de coût, soit pour des raisons techniques (par exemple utilisation d'une interface sans contact), soit pour les deux.

Une autre application possible est la télécarte de future génération, pour laquelle les contraintes de coût sont encore plus sévères que pour le porte-monnaie électronique.

Etat de la technique antérieure

De nombreux protocoles d'identification sans apport de connaissance sont connus. On peut citer entre autres les quatre protocoles suivants :

1) le protocole de FIAT-SHAMIR décrit dans : A. FIAT et A. SHAMIR, "How to prove yourself : Practical solutions to identification and signature problems", publié dans Advances in Cryptology ; Proceedings of CRYPTO'86, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, Berlin, 1987, pp. 186-194 ;

2) le protocole de GUILLOU-QUISQUATER décrit dans : L.C. GUILLOU et J.J. QUISQUATER, "A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory", publié dans Advances in Cryptology : Proceedings of EUROCRYPT'88, Lecture Notes in Computer

Science, vol. 330, Springer-Verlag, Berlin, 1988, pp. 123-128 ;

3) le protocole de SCHNORR décrit dans : C.P. SCHNORR, "Efficient identification and signatures for smart cards", publié dans Advances in Cryptology : Proceedings of CRYPTO'89, Lecture Notes in Computer Science, vol. 435, Springer-Verlag, Berlin, 1987, pp. 239-252 ;

4) le protocole de GIRAULT décrit dans la demande de brevet français FR-A-2 716 058.

De façon générale, la plupart des protocoles d'authentification sans apport de connaissance se déroulent en 4 étapes. On supposera, pour simplifier, que l'entité authentifiante, notée B, connaît déjà tous les paramètres publics caractéristiques de l'entité à authentifier, notée A, à savoir son identité, sa clé publique, etc... Les quatre étapes sont alors les suivantes :

Etape 1 :

A fournit à B au moins un engagement c, constitué soit par un paramètre x choisi au hasard par A, soit par une fonction pseudo-aléatoire h du paramètre x et, s'il y a lieu, du message à authentifier ou à signer : c=h(x,[M]), (la notation [M] exprime que M est optionnel).

Etape 2 :

B choisit au hasard un paramètre e appelé "question" et transmet e à A.

Etape 3 :

A fournit à B une réponse y, cohérente avec la question e, l'engagement c et la clé publique v de A.

Etape 4 :

B calcule x à partir des éléments y, e et v soit $x=\varphi(y,e,v)$ puis vérifie que : $c=h(\varphi(v,e,y),[M])$.

Dans certains protocoles, il y a un ou deux échanges supplémentaires entre A et B. Dans le cas d'une signature de message, les deux premiers échanges sont supprimés, et le paramètre e est choisi égal à c : A calcule successivement, et seul, c,e(c'est-à-dire c) et y.

Le nombre u de questions pouvant être choisies par B est directement relié au niveau de sécurité du protocole, lequel dépend de la probabilité de succès d'un imposteur (c'est-à-dire d'une entité C qui tente frauduleusement de se faire passer pour A). Ce niveau de sécurité, noté p, est caractérisé par un paramètre k, selon la relation $p=1-2^{-k}$. En d'autres termes, l'imposteur n'a qu'une chance sur 2^k de réussir son imposture. On peut montrer que, si le protocole repose sur un problème mathématique difficile, et si les engagements sont de longueur suffisante, alors il suffit que la longueur de u soit égale à k bits. En d'autres termes, la question doit être choisie dans l'ensemble $\{0, \ldots, 2^k-1\}$ (bornes incluses).

Dans l'état de la technique, k est égal à 32 bits, ce qui donne seulement une chance sur quatre milliards de réussir une imposture. Dans les applications où l'échec d'une identification peut avoir des conséquences très néfastes (poursuite judiciaire par exemple), cette longueur peut être réduite à quelques bits.

Dans leur version de base, aucun des protocoles mentionnés ne peut être mis en oeuvre dans une application à fortes contraintes, comme celles qui ont été évoquées plus haut, car les calculs requis ne peuvent être effectués par une carte à microcircuit non dotée d'un cryptoprocesseur.

Une première optimisation, due à FIAT et SHAMIR, concerne le nombre de bits échangés entre les deux entités. Elle consiste à utiliser une fonction de hachage lors du calcul de l'engagement. A elle seule, cette optimisation ne permet pas de diminuer le nombre de calculs effectués par l'entité authentifiée, car l'engagement continue d'être calculé par elle.

Pour diminuer ce nombre, il faut faire appel à un mode d'utilisation particulier, que l'on appelle mode à précalculs, consistant à calculer à l'avance des paramètres que l'on appellera pré-engagements et qui entrent dans le calcul des engagements. On peut aussi faire calculer des engagements par un serveur disposant d'une puissance de calcul supérieure, puis les stocker dans la carte à microcircuit de l'entité à authentifier. Au moment précis de la transaction électronique, la carte à microcircuit n'a plus alors à effectuer que des calculs rudimentaires. Ce mode d'utilisation est divulgué dans la demande FR-A-2 716 058 citée. Chaque pré-engagement est utilisé pour une et une seule transaction. Lorsque tous les pré-engagements ont été consommés par la carte, il est nécessaire d'en recalculer de nouveaux et de les stocker dans la carte (opération de rechargement).

La mémoire de données d'une carte à microcircuit à bas coût ne dépassant que rarement 8 Koctets, il est difficilement concevable de consacrer plus de 1 Koctet

au seul stockage des pré-engagements. Il est donc nécessaire de réduire autant que possible la taille de ces derniers, pour réaliser un maximum de transactions entre deux rechargements.

Dans tous ces procédés d'authentification, on peut définir une capacité de calcul qui est le nombre maximum de calculs que les moyens mis en œuvre peuvent effectuer en un temps raisonnable. Comme ces calculs sont binaires, on peut exprimer cette capacité sous forme d'une puissance de 2, par exemple sous la forme 2^N où N est un entier. Ce nombre n'est pas déterminé avec une extrême précision, mais est défini à quelques unités près. Par exemple, de nos jours, l'entier N est de l'ordre d'environ 80, c'est-à-dire qu'avec les moyens dont on dispose, la capacité est de 2^{80}, c'est-à-dire qu'on peut effectuer au maximum environ 2^{80} opérations dans un temps raisonnable.

Dans la version de base du procédé décrit dans la demande FR-A-2 716 058 citée, la taille des pré-engagements ou des engagements eux-mêmes est d'environ 2N bits, où le nombre N est pris égal à environ 80. La taille d'un pré-engagement est donc de l'ordre de 160 bits (elle est de 128 bits dans le document cité, où N est pris égal à 64). On peut donc stocker 50 engagements dans une mémoire de 1 Koctet, ce qui est relativement peu.

Dans une autre demande FR-A-2 752 122, il est décrit un procédé d'authentification permettant de réduire le nombre de bits à transmettre ou à stocker. La taille des pré-engagements ou des engagements peut être réduite à un peu plus de N bits (soit environ 88 avec N=80), ce qui permet de stocker plus de 90 pré-engagements dans une mémoire de 1 Koctet et de réduire

jusqu'à 18% des bits transmis lors de l'exécution du protocole.

Malheureusement, ce gain reste insuffisant pour de nombreuses applications, en particulier pour le porte-monnaie électronique. Beaucoup de transactions peuvent ne concerner que de très petit montants (transports en commun, parcmètres, télécommunications locales, etc...), et l'utilisateur doit pouvoir effectuer des transactions jusqu'à épuisement du solde, sans être limité par aucune autre considération. Dans ce contexte, un minimum de 150 à 200 transactions sans rechargement semble devoir être exigé, ce que les procédés connus ne permettent pas.

C'est justement le but de la présente invention de réduire encore la taille des pré-engagements et, optionnellement, des engagements eux-mêmes. Selon l'invention, on peut descendre à environ 48 bits, ce qui permet de stocker 170 pré-engagements dans une mémoire de 1 Koctet. Dans certaines applications, cette taille peut être encore inférieure et par exemple tomber à 32 bits, ce qui permet de stocker 256 pré-engagements.

L'invention rend ainsi possible l'exécution rapide d'un algorithme d'identification ou d'authentification de message ou de signature de message, dans une carte à microcircuit standard à bas coût, pour des applications telles que le porte-monnaie électronique ou la télécarte de future génération.

Exposé de l'invention

L'invention repose sur l'observation suivante : la capacité de calcul est très fortement diminuée (typiquement 2^{16} au lieu de 2^{80}) si on contraint le

fraudeur à effectuer les calculs dans un laps de temps petit et avec des moyens de calcul réduits.

Partant de cette observation, l'invention propose de mesurer le temps Δt mis par l'entité à authentifier pour répondre à l'entité authentifiante et de limiter ce temps à une valeur maximum Δt_{max}.

Dans le laps de temps Δt_{max}, les moyens mis en œuvre ont une capacité de calcul égale à 2^P (selon les considérations développées plus haut). Ce nombre 2^P est naturellement inférieur au nombre 2^N en raison de la contrainte qui pèse sur le temps accordé pour effectuer ces calculs. L'invention propose alors de prendre comme taille des pré-engagements ou des engagements le nombre k+P ou un nombre supérieur mais restant inférieur à k+N. Typiquement, le nombre P peut être de l'ordre de 16, de sorte que si k=32, la taille du pré-engagement ou de l'engagement sera de 32+16 soit 48 bits ou un peu plus (à comparer avec les 128 ou 88 bits dans les deux demandes de brevet déjà citées).

Deux options s'offrent alors :

- une première option dans laquelle on allonge la question e (qui, dans l'art antérieur, possède une taille de k bits), ce qui, typiquement, donne une taille d'environ 64 bits ;
- une seconde option dans laquelle on ajoute au protocole un échange préliminaire au cours duquel B envoie un nombre aléatoire w à A, (typiquement 32 bits), lequel nombre w constitue un paramètre supplémentaire pris en compte pour le calcul de l'engagement c : $c=h(\alpha,w,[M])$; l'intervalle de temps Δt à mesurer est alors celui qui s'écoule entre

l'envoi de l'échange préliminaire et la réception des paramètres e et y. La question posée e peut garder alors la taille de k bits.

Pour une signature de message, cette seconde option doit être obligatoirement retenue. L'intérêt de cette seconde option est que la taille de la question e reste réduite. Or, dans certains protocoles (notamment ceux de FIAT-SHAMIR et de GUILLOU-QUISQUATER), le temps de calcul de la réponse y dépend beaucoup de la longueur de e, alors que le temps de calcul de l'engagement c dépend très peu de la longueur de w. Pour ces protocoles, la seconde option permet donc de diminuer la taille des engagements sans augmenter notablement le temps d'exécution du protocole. Par ailleurs, cette seconde option est la seule possible dans le cas de la signature de message, puisqu'il n'y a plus de question à proprement parler.

Le niveau de sécurité du protocole selon l'invention (c'est-à-dire la probabilité minimale de détection d'un imposteur) est équivalent à celui des protocoles connus ($1-2^{-k}$), alors que la longueur des pré-engagements ou des engagements est divisée par presque quatre. On peut démontrer cette équivalence des niveaux de sécurité de la manière suivante. Soit C un fraudeur, qui chercherait à se faire passer pour A (ou à faire croire que le message M provient de A). C ne connaît évidemment pas la clé secrète de A. Il peut mettre en oeuvre essentiellement trois stratégies, que l'on peut désigner par "fraude par devinette", "fraude en temps réel" (effectuée pendant la transaction) et "fraude en temps différé" (effectuée avant la

transaction), stratégies qui peuvent d'ailleurs être combinées :

a) fraude par devinette :

- première option : C devine la valeur de la question e en la choisissant au hasard, choisit la réponse y au hasard et calcule $c=h(\varphi(v,e,y),[M])$. Puis il commence la transaction avec cette valeur de c. Il ne réussira que s'il a bien deviné e, donc avec une probabilité de 2^{-64}.

- seconde option : C devine la valeur de la question e en la choisissant au hasard, choisit la réponse y au hasard et calcule $c=h(\varphi(v,e,y),w,[M])$. Il ne peut le faire qu'une fois connu w, donc pendant la transaction. Puis il continue la transaction avec cette valeur de c. Il ne réussira que s'il a bien deviné e, donc avec une probabilité de 2^{-64}.

b) fraude en temps réel :

Après avoir envoyé une valeur (au hasard) de c, et reçu une valeur de e, C recherche par essais exhaustifs une valeur de y qui satisfasse l'équation de vérification $c=h(\varphi(v,e,y),[M])$. Puisqu'il peut effectuer un maximum de 2^P essais, et que le nombre de valeurs possibles de c est 2^{k+P}, sa probabilité de réussite est $1/2^k$, comme souhaité.

c) fraude en temps différé :

- première option : C calcule un grand nombre de valeurs de c à partir de diverses valeurs de y et e. Puisqu'il peut en calculer un maximum de 2^N, il y aura pour chaque valeur possible de c environ 2^{N-P-k} valeurs correspondantes de y et de e. C choisit une quelconque de ces valeurs, stocke les valeurs de y et e correspondantes et entame le protocole. Puisqu'il y a 2^{N-P} valeurs possibles de e, la probabilité que C ait

stocké la valeur qui lui est envoyée par B est de nouveau inférieure à $1/2^k$, comme souhaité.

- seconde option : le calcul est essentiellement le même que pour la première option, puisque la taille totale des deux nombres aléatoires w et e est égale à la taille de e dans la seconde option.

De façon précise, la présente invention a donc pour objet un procédé d'authentification mettant en oeuvre une première entité dite à "authentifier" (A) et une seconde entité dite "authentifiante" (B), ce procédé comprenant les opérations suivantes :

- l'entité à authentifier (A) envoie au moins un engagement c à l'entité authentifiante (B), cet engagement ayant une certaine taille comptée en nombre de bits,
- l'entité authentifiante (B) reçoit cet engagement c, choisit au hasard un nombre e appelé "question" et envoie cette question e à l'entité à authentifier (A),
- l'entité à authentifier (A) reçoit la question e, effectue des calculs utilisant cette question e, le résultat de ces calculs constituant une réponse y et envoie cette réponse y à l'entité authentifiante (B),
- l'entité authentifiante (B) reçoit la réponse y, effectue un calcul utilisant cette réponse y et vérifie que ce calcul redonne l'engagement reçu c,

un niveau de sécurité égal à $1-2^{-k}$ étant obtenu pour cette authentification où k est un entier que l'on se fixe selon le niveau de sécurité désiré,

ce procédé étant caractérisé en ce que l'entité authentifiante (B) mesure l'intervalle de temps (Δt) s'écoulant entre l'instant où elle s'adresse à l'entité à authentifier (A) et l'instant où elle reçoit la réponse de l'entité à authentifier (A), et elle vérifie que l'intervalle de temps mesuré (Δt) est inférieur à un intervalle de temps déterminé Δt_{max}, et en ce que, l'entité à authentifier (A) ayant une capacité de calcul d'environ 2^P dans ledit intervalle de temps déterminé (Δt_{max}), l'engagement c utilisé par l'entité à authentifier (A) possède une taille égale au moins à (k+P) bits.

Dans cette définition, il faut comprendre que la taille peut être soit égale à (k+P) bits, soit être supérieure de quelques unités à ce nombre.

Dans un mode de mise en œuvre particulier, l'entité à authentifier (A) calcule l'engagement à partir d'un pré-engagement calculé à l'avance, lequel possède une taille égale à au moins (k+P) bits. Mais l'entité à authentifier peut également calculer l'engagement par tirage au hasard d'un nombre et calculs à partir de ce nombre.

Dans une autre variante de mise en œuvre, l'entité authentifiante (B), dans une opération préliminaire, choisit au hasard un nombre w et envoie ce nombre w à l'entité à authentifier (A) laquelle utilise ce nombre w pour constituer l'engagement, la question e posée par l'entité authentifiante (B) possédant un nombre de bits égal à k, l'intervalle de temps mesuré étant l'intervalle compris entre l'instant où l'entité authentifiante (B) envoie le nombre w à l'entité à authentifier (A) et l'instant où l'entité

authentifiante (B) reçoit la réponse y de l'entité à authentifier (A).

La présente invention a également pour objet un procédé de signature de message dans lequel on met en oeuvre une première entité dite "signataire" (A) et une seconde entité dite "authentifiante" (B), ce procédé comprenant les opérations suivantes :

- l'entité signataire (A) calcule un nombre e fonction du message à signer et calcule un nombre y appelé réponse, et envoie cette réponse à l'entité authentifiante (B),
- l'entité authentifiante (B) reçoit la réponse y, effectue un calcul utilisant cette réponse y et vérifie que ce calcul redonne le nombre e,

un niveau de sécurité égal à $1-2^{-k}$ étant obtenu pour cette signature où k est un entier que l'on se fixe selon le niveau de sécurité désiré,

ce procédé étant caractérisé en ce que :

- l'entité signataire (A) calcule un nombre e dont la taille est égale à au moins (k+P) bits où 2^P représente la capacité de calcul de l'entité à authentifier (A) dans un intervalle de temps fixé (Δt_{max}),
- dans une opération préliminaire, l'entité authentifiante (B) choisit au hasard un nombre w et envoie ce nombre w à l'entité signataire (A) laquelle utilise ce nombre w pour constituer le nombre e,
- l'entité authentifiante (B) mesure l'intervalle de temps Δt qui s'écoule entre l'instant où elle envoie le nombre w à l'entité signataire

(A) et l'instant où elle reçoit la réponse y de l'entité signataire (A), et elle vérifie que l'intervalle mesuré Δt est inférieur à l'intervalle de temps fixé Δt_{max}.

Là encore, l'entité signataire peut calculer le nombre e à partir d'un préengagement calculé à l'avance, lequel possède une taille égale à au moins (k+P) bits, à quelques unités près.

Description détaillée de modes particuliers de réalisation

Dans la description qui suit, on supposera que l'invention s'applique dans le cadre de la technique divulguée dans la demande de brevet FR-A-2 716 058 déjà citée, technique dans laquelle les multiplications modulaires sont supprimées, notamment dans l'opération de l'étape 3. Ce type d'opérations n'a donc pas besoin d'être prévu dans la carte à microcircuit quand le mode à précalculs est utilisé. Naturellement, cet exemple ne limite pas la portée de l'invention qui peut être utilisée avec des protocoles à multiplications modulaires.

Les protocoles conformes à la demande citée sont basés sur la difficulté de calculer les logarithmes discrets. Les paramètres universels (c'est-à-dire partagés par tous les utilisateurs) sont :

- un grand nombre composé n,
- un entier α (la "base"),
- quatre paramètres t, k, u, z, où k est le paramètre de sécurité.

La longueur recommandée pour n est (au moins) de 512 bits, et de préférence 768 bits ou plus. Une valeur

typique du paramètre de sécurité k est 32. Le paramètre u désigne le nombre de questions possibles (on a donc $u=2^k$). Une valeur typique de la longueur de t est 160 bits. Une valeur typique de la longueur de z est 64 bits.

La clé secrète d'un utilisateur est un entier s inférieur à t. Sa clé publique est : $v=\alpha^{-s} \pmod n$.

Le protocole d'authentification de base, divulgué dans cette demande antérieure, est le suivant :

1. A choisit au hasard un entier r dans {0...tuz-1}, calcule $x=\alpha^r \pmod n$ et envoie c à B.

2. B choisit au hasard un élément e dans {0 ... 2^k-1} et envoie e à A.

3. A calcule y=r+se et envoie y à B.

4. B vérifie que $x=\alpha^y v^e \pmod n$.

On remarque qu'un imposteur (qui par hypothèse ignore s) peut tromper un vérificateur avec une probabilité égale à 2^{-k}, en choisissant un entier y, un élément e et en calculant x comme dans l'étape 4. Comme on peut prouver que, si le problème du logarithme discret est difficile, il ne peut substantiellement améliorer cette probabilité, le niveau de sécurité est donc égal à $1-2^{-k}$.

Afin de diminuer le nombre de bits transmis, on peut, comme l'on suggéré FIAT et SHAMIR, prendre comme engagement c=h(x) où h est une fonction pseudo-aléatoire. L'équation de vérification de l'étape 4 devient alors :

$$c=h(\alpha^y v^e \pmod n).$$

Si l'on veut, de surcroît, authentifier un message M, alors on introduit M dans le calcul de l'engagement : $c=h(x,M)$.

Afin de conserver un niveau de sécurité égal à $1-2^{-k}$, il est nécessaire, toutes choses égales par ailleurs, que la longueur de c soit au moins 160 bits.

Ce rappel étant effectué, on peut décrire le protocole correspondant selon la présente invention dans une variante utilisant la première option. On prendra N=80 et P=16 et en supposant que les longueurs du pré-engagement et de l'engagement sont toutes deux réduites à leur minimum, c'est-à-dire à 48 bits, cette réduction étant compensée par une augmentation de la longueur de e, qui passe à 64 bits. De plus, à l'étape 4, un contrôle du temps mis par A est effectué par B. De la sorte, le niveau de sécurité du protocole modifié reste égal à $1-2^{-k}$. Les étapes du procédé selon l'invention deviennent alors :

1. A choisit au hasard un entier r dans {0 ...tuz-1}, calcule $x=\alpha^r \pmod n$, puis éventuellement $c'=f(x)$ qui appartient à $\{0 \ldots 2^{48}-1\}$, puis $c=h(x,w,[M])$, ou $c=h(x',w,[M]$, qui appartient à $\{0 \ldots 2^{48}-1\}$ et envoie c à B.

2. B choisit au hasard un élément e dans $\{0 \ldots 2^{64}-1\}$ et envoie e à A.

3. A calcule $y=r+se$ et envoie y à B.

4. B vérifie que $c=h(\alpha^y v^e \pmod n,[M])$ ou $c=h(f(\alpha^y v^e \pmod n),[M])$ et que l'intervalle de temps entre l'émission de l'étape 2 et la réception de l'étape 3 est inférieur à une ou deux secondes.

L'invention est particulièrement bien adaptée à un tel protocole de base, car elle n'entraîne aucun changement des paramètres universels principaux, à savoir n et α, ni même des paramètres individuels (clés secrète et publique de l'utilisateur). En revanche, elle implique un allongement de e, car u est maintenant égal à 2^{64} (mais ceci ne serait plus vrai si l'on adoptait la seconde option).

Par ailleurs et surtout, l'invention est particulièrement utile dans le mode à précalculs, puisque les pré-engagements ont une taille réduite à 48 bits. Certes, il faut au préalable stocker non seulement les pré-engagements mais aussi les valeurs de r correspondantes. Cependant, il est possible d'éviter cela en générant ces nombres à l'aide d'un générateur pseudo-aléatoire contenu dans le dispositif de sécurité de A, comme il est décrit dans la demande FR-A-2 716 058 déjà citée.

Si l'on opte pour la seconde option, le procédé comprend une étape supplémentaire et préalable notée 0 et devient :

0. B choisit au hasard un nombre aléatoire w dans $\{0 \ldots 2^{32}-1\}$ et l'envoie à A.

1. A choisit au hasard un entier r dans {0 ... tuz-1}, calcule $x=\alpha^r \pmod n$ puis éventuellement $x'=f(x)$ qui appartient à $\{0 \ldots 2^{48}-1\}$, puis c=h(x,w,[M]), ou c=h(x',w,[M] qui appartient à $\{0 \ldots 2^{48}-1\}$, et envoie c à B.

2. B choisit au hasard un élément e dans {0 ... $2^{32}-1$} et envoie e à A.

3. A calcule y=r+se et envoie y à B.

4. B vérifie que $c=h(\alpha^y v^e \pmod n, w, [M])$ ou $c=h(f(\alpha^y v^e \pmod n), w, [M]))$ et que l'intervalle de temps entre l'émission de l'étape 0 et la réception de l'étape 3 est inférieur à une ou quelques secondes.

Enfin, le protocole de signature sera :

0. B choisit au hasard un nombre aléatoire w dans {0 ... $2^{64}-1$} et l'envoie à A.

1. A choisit au hasard un entier r dans {0 ...tuz-1} et calcule $x=\alpha^r \pmod n$ puis éventuellement $x'=f(x)$, qui appartient à {0 ... $2^{48}-1$}.

2. A calcule $e=h(x,w,[M])$ qui appartient à {0 ...$2^{48}-1$}.

3. A calcule y=r+se et envoie (e,y) à B.

4. B vérifie que $e=h(\alpha^y v^e \pmod n, w, [M])$ et que l'intervalle de temps entre l'émission de l'étape 0 et la réception de l'étape 3 est inférieur à une ou quelques secondes.

REVENDICATIONS

1. Procédé d'authentification mettant en oeuvre une première entité dite à "authentifier" (A) et une seconde entité dite "authentifiante" (B), ce procédé comprenant les opérations suivantes :

- l'entité à authentifier (A) envoie au moins un engagement c à l'entité authentifiante (B), cet engagement ayant une certaine taille comptée en nombre de bits,
- l'entité authentifiante (B) reçoit cet engagement c, choisit au hasard un nombre e appelé "question" et envoie cette question e à l'entité à authentifier (A),
- l'entité à authentifier (A) reçoit la question e, effectue des calculs utilisant cette question e, le résultat de ces calculs constituant une réponse y et envoie cette réponse y à l'entité authentifiante (B),
- l'entité authentifiante (B) reçoit la réponse y, effectue un calcul utilisant cette réponse y et vérifie que ce calcul redonne l'engagement reçu c,

un niveau de sécurité égal à $1-2^{-k}$ étant obtenu pour cette authentification où k est un entier que l'on se fixe selon le niveau de sécurité désiré,

ce procédé étant caractérisé en ce que l'entité authentifiante (B) mesure l'intervalle de temps (Δt) s'écoulant entre l'instant où elle s'adresse à l'entité à authentifier (A) et l'instant où elle reçoit la réponse de l'entité à authentifier (A), et elle vérifie que l'intervalle de temps mesuré (Δt) est inférieur à

un intervalle de temps déterminé Δt_{max}, et en ce que, l'entité à authentifier (A) ayant une capacité de calcul d'environ 2^P dans ledit intervalle de temps déterminé (Δt_{max}), l'engagement c utilisé par l'entité à authentifier (A) possède une taille égale à au moins (k+P) bits.

2. Procédé selon la revendication 1, dans lequel l'entité à authentifier (A) calcule l'engagement à partir d'un pré-engagement calculé à l'avance, lequel possède une taille égale au moins à (k+P) bits.

3. Procédé d'authentification selon l'une quelconque des revendications 1 et 2, dans lequel le nombre P est pris égal à 16 et le nombre k à 32, le pré-engagement ou l'engagement ayant ainsi une taille égale au moins à 48 bits.

4. Procédé d'authentification selon la revendication 1, dans lequel la question e posée par l'entité authentifiante (B) possède un nombre de bits supérieur à k.

5. Procédé selon la revendication 4, dans lequel le nombre k étant égal à 32 la question posée e par l'entité authentifiante (B) possède un nombre de bits égal à environ 64.

6. Procédé d'authentification selon la revendication 1, dans lequel l'entité authentifiante (B), dans une opération préliminaire, choisit au hasard un nombre w et envoie ce nombre w à l'entité à authentifier (A) laquelle utilise ce nombre w pour

constituer l'engagement c, la question e posée par l'entité authentifiante (B) possédant un nombre de bits égal à k, l'intervalle de temps (Δt) étant mesuré entre l'instant où l'entité authentifiante (B) envoie le nombre w à l'entité à authentifier et l'instant où l'entité authentifiante (B) reçoit la réponse y de l'entité à authentifier (A).

7. Procédé d'authentification selon la revendication 6, dans lequel le nombre w préalablement fourni par l'entité authentifiante (B) à l'entité à authentifier (A) possède environ 32 bits, l'engagement ayant une taille égale au moins à 48 bits, la question e posée par l'entité authentifiante (B) ayant un nombre de bits égal à environ 32.

8. Procédé d'authentification selon l'une quelconque des revendications 1 à 7, dans lequel l'entité à authentifier (A) introduit un message (M) dans l'engagement qu'elle constitue, l'authentification portant alors aussi sur le message (M).

9. Procédé de signature de message dans lequel on met en oeuvre une première entité dite "signataire" (A) et une seconde entité dite "authentifiante" (B), ce procédé comprenant les opérations suivantes :

- l'entité signataire (A) calcule un nombre e fonction du message à signer et calcule un nombre y appelé réponse, fonction du nombre e et envoie cette réponse à l'entité authentifiante (B),

- l'entité authentifiante (B) reçoit la réponse y, effectue un calcul utilisant cette réponse y et vérifie que ce calcul redonne le nombre e,

un niveau de sécurité égal à $1-2^{-k}$ étant obtenu pour cette signature où k est un entier que l'on se fixe selon le niveau de sécurité désiré,

ce procédé étant caractérisé en ce que :

- l'entité signataire (A) calcule un nombre e dont la taille est égale au moins à (k+P) bits où 2^P représente la capacité de calcul de l'entité à authentifier (A) dans un intervalle de temps fixé (Δt_{max}),
- dans une opération préliminaire, l'entité authentifiante (B) choisit au hasard un nombre w et envoie ce nombre w à l'entité signataire (A) laquelle utilise ce nombre w pour constituer le nombre e,
- l'entité authentifiante (B) mesure l'intervalle de temps Δt qui s'écoule entre l'instant où elle envoie le nombre w à l'entité signataire (A) et l'instant où elle reçoit la réponse y de l'entité signataire (A), et elle vérifie que l'intervalle mesuré Δt est inférieur à l'intervalle de temps fixé Δt_{max}.

10. Procédé selon la revendication 9, dans lequel l'entité signataire (A) calcule le nombre e à partir d'un préengagement calculé à l'avance, lequel possède une taille égale au moins à (k+P) bits.

11. Procédé de signature de message selon les revendications 9 ou 10, dans lequel le nombre P est

pris égal à 16 et le nombre k à 32, le préengagement ou le nombre e ayant ainsi une taille égale au moins à 48 bits.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2792142

N° d'enregistrement national

FA 574264
FR 9904398

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP 0 697 687 A (NIPPON TELEGRAPH & TELEPHONE) 21 février 1996 (1996-02-21) * abrégé * * colonne 4, ligne 20 - colonne 5, ligne 36 * * revendications 1,2 * * figures 1A,1B,1C,2,3 *	1-4,6,8, 9
A	FR 2 716 058 A (FRANCE TELECOM ;POSTE) 11 août 1995 (1995-08-11) cited by the applicant * abrégé * * page 1, ligne 8 - ligne 20 * * page 4, ligne 32 - page 7, ligne 31 * * revendication 1 *	9-11

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)

H04L

1

Date d'achèvement de la recherche	Examinateur
10 janvier 2000	Gautier, L

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)